REMARKS/ARGUMENTS

1.) Claim Amendments

Claim 28 has been cancelled and claims 24, 25, 27, 30-32 and 35-39 have been amended; no new matter has been added. Accordingly, claims 24-27 and 29-46 remain pending in the application.

2.) Claim Rejections – 35 U.S.C. §101

The Examiner rejected claims 24-40 on the asserted basis that those claims are directed to non-statutory subject matter on the asserted basis that the claims recite "means for" claims limitations without "integrating a machine (*e.g.*, a computer)." The Applicants disagree. The functions performed by the various "means for" elements, as authorized under §112, Paragraph 6, are disclosed as being performed by conventional telecommunications network elements known to those skilled in the art as various general or specific-purpose computers. Therefore, the claims do recite statutory subject matter.

3.) Claim Rejections – 35 U.S.C. §112, 2nd ¶

The Examiner rejected claims 24-36 and 37-40 as being indefinite on the asserted basis that they recite "means for" claim elements with no structure disclosed in the specification. As noted *supra*, the functions performed by the various "means for" elements, as authorized under §112, Paragraph 6, are disclosed as being performed by conventional telecommunications network elements known to those skilled in the art as various general or specific-purpose computers. Therefore, the claims are not indefinite.

4.) Claim Rejections – 35 U.S.C. § 102(e)

The Examiner rejected claim 37 as being anticipated by Jin, *et al.* (U.S. Patent No. 6,643,782). The Applicants traverse the rejections.

First, it is to be remembered that anticipation requires that the disclosure of a single piece of prior art reveals **every** element, or limitation, of a claimed invention. Furthermore, the limitations that must be met by an anticipatory reference are those set

forth in each statement of function in a claims limitation, and such a limitation cannot be met by an element in a reference that performs a different function, even though it may be part of a device embodying the same general overall concept. Whereas Jin fails to anticipate each and every limitation of claim 37, that claim is not anticipated thereby.

The Examiner states that Jin discloses (col. 1 lines 15-21) a user equipment arranged to carry out an authentication procedure with a core network, and arranged to access a telecommunication service network via an access network unable to provide data origin authentication. Jin, however, does not disclose that the access network is unable to provide data origin authentication, as recited in claim 37. In fact, Jin discloses a Service Selection Gateway (SSG) for accessing a private area interposed between a Network Access Server (NAS) and an Authentication, Authorization and Accounting server (AAA) provided for authentication purposes. Such interposition implies that the SSG is aware of the signaling exchanged between the user and the AAA server and, consequently, the SSG is a witness of the authentication of the user, which is apparently interpreted by the Examiner as an entry point to a service network.

The scenario addressed by the Applicants' invention, however, is where there is no intercepting node, such as SSG, and the access to the home core network is handled by a direct communication between NAS and AAA Server, whereas the access to the service network is neither handled by, nor involving, such NAS and Authentication Server; *i.e.,* it does not involve an entity (*e.g.*, the SSG) previously involved in the authentication of the user by the core network. Therefore, there is no incentive for a skilled person to apply this teaching to provide single sign-on services in scenarios where the access network is unable to provide data origin authentication.

Furthermore, the fact of interposing the SSG between the NAS and the AAA does not imply the establishment of a secure tunnel. Interposing the SSG between the NAS and the AAA, as asserted by the Examiner, neither anticipates a user equipment having means for establishing a secure tunnel with the Secure Service Entry Point of the service network through the access network, the secure tunnel making use of an outer IP address assigned to the user by the access network for addressing the user, nor means for receiving an internal IP address assigned by the service network and

included as an inner IP address within the tunneled traffic to identify the user in the service network, all of which are recited in claim 37.

Moreover, regarding IP addresses assigned to the user equipment, Jin teaches (col. 2, lines 40-51) that an IP address is assigned to the user either by the NAS or by the AAA. This IP address assigned to the user, according to Jin, can be interpreted as the "outer IP address assigned to the user by the access network for addressing the user" as recited in claim 37. Jin, however, does not teach the assignment of *another* IP address to the user by the service network; *i.e.*, Jin does not teach the "inner IP address within the tunneled traffic to identify the user in the service network" that is recited in claim 37. The Examiner, in fact, acknowledges this deficiency in the teachings of Jin in the stated reasons for rejection of claim 24 (Office Action, Section 11), wherein the Examiner relies on the further teachings of Montenegro (U.S. Patent No. 6,571,289).

Finally, if the SSG as taught by Jin is interpreted as the entry point to the service network according to the Applicants' invention, Jin would still need to disclose that the SSG assigns another IP address, an "inner" IP address, to be used to identify the user in the service network. Nothing in Jin, however, suggests a user equipment having means for establishing a secure tunnel with the Secure Service Entry Point of the service network through the access network, the secure tunnel making use of an outer IP address assigned to the user by the access network for addressing the user, and means for receiving an internal IP address assigned by the service network and included as an inner IP address within the tunneled traffic to identify the user in the service network. Therefore, Jin fails to anticipate claim 37.

5.) Claim Rejections – 35 U.S.C. § 103(a)

The Examiner rejected claims 24-30 and 41-45 as being unpatentable over Jin, *et al.* (U.S. Patent No. 6,643,782) in view of Montenegro (U.S. Patent No. 6,571,289); and claims 31-36 and 46 as being unpatentable over Jin in view of Montenegro and further in view of Schneider, *et al.* (U.S. Patent No. 6,105,027). The Applicants traverse the rejections.

Regarding claim 24, the Examiner acknowledges that Jin does not disclose establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic. As noted *supra*, the Examiner's acknowledgement confirms that claim 37 is novel in view of the teachings of Jin. Montenegro, however, fails to overcome the deficiencies of Jin.

Montenegro discloses a plurality of tunnel segments composing a chain of a registration request from a mobile node to a private network. More particularly, Montenegro discloses (see: col. 4 lines 14-36) that when a correspondent node, whose address is CN, desires to send a packet of information to a mobile node, whose address is MN, in a private network, the correspondent node will compose a packet with a source address of CN and a destination address of MN. This packet is intercepted by a Home Agent in the private network, whose address is HA, and the Home Agent forwards such packet to a Gateway, whose address is GW, by pre-pending an additional header with a source address of HA and a destination address of GW. The Gateway receives such packet and strips off the added header to recover the original packet with source address of CN and destination address of MN, and encounters that such MN address has a binding in the GW with an address of a Foreign Agent, whose address is FA. This binding makes the Gateway pre-pend its own new header with source address of GW and destination address of FA. The Foreign Agent receiving such packet also strips off the latest header and recovers the original packet with source address of CN and destination address of MN. From this teaching in Montenegro, it can be seen that the original packet has a unique header with a source address of CN and a destination address of MN when submitted between the correspondent node and the Home Agent as well as when submitted between the Foreign Agent and the mobile node in the private network; and the original packet has an additional header pre-pended to the original packet, with source address of HA and a destination address of GW, when submitted between the Home Agent and the Gateway, and another additional header pre-pended to the original packet, with source

address of GW and a destination address of FA, when submitted between the Gateway and the Foreign Agent. In other words, Montenegro discloses more than one source address and more than one destination address for a same unique packet, wherein the more than one source address and wherein the more than one destination address always correspond to *different* entities.

Montenegro thus fails to anticipate two different IP address corresponding to the *same* entity accompanying the packet and used for different purposes. More specifically, Montenegro fails to disclose an outer IP address assigned to the user by the access network for addressing the user and an internal IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic. Therefore, even if disclosing secure tunnels, Montenegro fails to teach means for establishing a secure tunnel with a user from a Secure Service Entry Point when receiving access credentials through an access network by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic.

Accordingly, claim 24 is not obvious over Jin in view of Montenegro. Similarly, whereas claim 41 recites analogous limitations, it is also not obvious. Furthermore, whereas claims 25-27 and 29-36 are dependent from claim 24 and claims 42-46 are dependent from claim 41, and include the limitations of their respective base claims, they are also not obvious in view of those references.

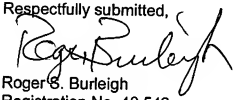
* * *

CONCLUSION

In view of the foregoing amendments and remarks, the Applicants believe all of the claims currently pending in the Application to be in a condition for allowance. The Applicants, therefore, respectfully request that the Examiner withdraw all rejections and issue a Notice of Allowance for claims 24-27 and 29-46.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Roger S. Burleigh
Registration No. 40,542

Date: December 9, 2008

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com